[redacted]

23-mj-5550-JGD

AFFIDAVIT OF SPECIAL AGENT/TASK FORCE OFFICER

I, Task Force Officer John Moynihan, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am presently a Boston Police Department (BPD) Detective, assigned to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Boston Field Division II, as a Task Force Officer (TFO). I am deputized by the United States Marshals Service (USMS) as a special deputy with the Violent Crimes Gun Task Force. I have been a sworn Boston Police Officer since 2008.

2. Before joining the BPD, I served as an Infantry Officer in the United States Army. While in the Army, I attended and completed the infantry officer's basic course, Army Airborne School, and Army Ranger School. In June 2009, I completed the Boston Police Academy. Since then, I have served in many assignments, including but not limited to patrol, Anti-Crime, Youth Violence Strike Force, and the Fugitive Apprehension Unit.

3. I have written and/or participated in the execution of numerous search warrants resulting in the seizure of large quantities of firearms, United States currency, records of firearms, monetary transactions, and the transportation and laundering of firearm proceeds. I have participated in the debriefing of numerous defendants, informants, and witnesses who had personal knowledge regarding firearm trafficking organizations. I have participated in all aspects of firearms investigations, including conducting surveillance, executing searches pursuant to court-ordered search warrants, executing arrests, and participating in court-authorized Title III wiretaps of cellular phones. I have received extensive specialized training in the field of firearm identification, investigation, and enforcement. In addition, I have attended and completed the two-week DEA basic narcotics investigator course, and during my time with BPD, I participated in numerous narcotics-related arrests.

4. Based on my training and experience, I am familiar with firearm traffickers' methods of operation, including methods used by them to distribute, store, and transport firearms and to collect, expend, account for, transport, and launder proceeds from illegal firearms. I am also familiar with the manner in which firearms traffickers use personal and rented cars and trucks, common carriers, mail and private delivery services, and a variety of other motor vehicles to (a) meet with co-conspirators, customers, and suppliers; (b) transport, distribute, and purchase firearms; (c) transport funds; and (d) transport the proceeds of these transactions.

5. I submit this affidavit in furtherance of an ongoing criminal investigation into Cordell Miller ("MILLER"), D.O.B. XX/XX/1996, SSN: XXX-XXX-8221 concerning violations of federal law including, Trafficking in Firearms and conspiracy to do so, in violation of 18 U.S.C. § 933(a)(3), Felon in Possession of Firearms and Ammunition, in violation of 18 U.S.C. § 922(g)(1); Aiding and Abetting, in violation of 18 U.S.C. § 2; Distribution and Possession with the Intent to Distribute Controlled Substances, in violation of 21 U.S.C. §841; and Conspiracy to Distribute and Possess with the Intent to Distribute Controlled Substances, in violation of 21 U.S.C. §846; hereinafter, the "TARGET OFFENSES."

6. This affidavit is being submitted in support of an application for a criminal complaint for MILLER and a search warrant to search the person of MILLER, his residence at 85 Evergreen Drive, Haverhill, MA (the "TARGET RESIDENCE"), and MILLER's motor vehicle, a gray 2020 Honda Civic, bearing MA registration 9YE112 ("TARGET VEHICLE") as described in attachments A-1, A-2, and A-3. There is probable cause to believe that the person of MILLER, the TARGET RESIDENCE and TARGET VEHICLE contain evidence, fruits, and instrumentalities of the TARGET OFFENSE, as described in Attachment B.

7. I submit this affidavit for the limited purpose of establishing probable cause for the requested search warrant and criminal complaint. Accordingly, I have not included each and every fact known to me, and other law enforcement officers involved in this investigation. As a result of my personal participation in the investigation, review of reports submitted by other law enforcement personnel, and my consultations with other law enforcement officers, I am familiar with this investigation.

BACKGROUND OF INVESTIGATION

8. I received uncorroborated information within the past few months from a known source, who wishes to remain anonymous, hereinafter, the known source will be referred to as ("CS"), that MILLER was trafficking firearms and ammunition in and outside of the City of Boston. The CS described MILLER as approximately 5 feet 11 inches, 265 pounds, with long black braids. The CS further stated that MILLER utilizes the cellular telephone number XXX-XXX-0335 to arrange meetings and to coordinate the subsequent locations where he sells firearms and ammunition.

9. Based on investigative techniques and the use of investigative databases, this Investigator was able to locate MILLER, D.O.B. XX/XX/1996, and SSN: XXX-XX-8221, and learned that the TARGET VEHICLE is registered to MILLER at an address in Haverhill, MA. Over the course of the past few months, investigators conducted surveillance at MILLER's address in Haverhill and observed his activities, including entering and exiting the address, as well as operating the TARGET VEHICLE on multiple occasions. This Investigator was able to identify MILLER based on his photograph from the Registry of Motor Vehicle (RMV) database. A Criminal Justice Information System (CJIS) query revealed that MILLER was convicted of

multiple felony charges. Specifically, MILLER has prior convictions for assault and battery, larceny, and breaking and entering, for which he was sentenced to one year committed in 2017.

10. In the last several months, ATF has made controlled firearm purchases from MILLER using an ATF Confidential Informant (CI), hereinafter referred to as "the CI."[1,2] Further, ATF has made drug purchases that were arranged/facilitated by MILLER through the CI.

First Controlled Purchase

11. On a date in August 2023, the CI contacted MILLER at (XXX-XX5-0335), to purchase cocaine. MILLER agreed and told the CI to meet him at Brewer Avenue in Brockton, Massachusetts. Prior to the sale, the CI met with investigators at a prearranged location. The CI was searched for contraband and was provided with audio/video recording devices along with U.S.

[1] The CI is cooperating for both financial consideration and in hopes for leniency in an open federal investigation in another district. The CI has cooperated reliably since his arrest in approximately 2020 on drug related charges, reportedly conducting more than 100 controlled purchases of evidence on behalf of ATF, which have been found reliable by his controlling ATF agents in that judicial district who monitored the transactions and debriefed the CI for information. Given his successful cooperation, a Judge of that district authorized the CI to come to the District of Massachusetts for the purposes of continuing to work as a Confidential Informant for ATF. The CI has an extensive criminal history including convictions for robbery and drug distribution and is working in part for consideration in a federal drug distribution case. Since his arrival in the District of Massachusetts, the CI has participated reliably in approximately twenty controlled purchases and has reliably reported on his observations, which ATF has corroborated whenever possible.

[2] I will refer to all CI's as male, regardless of their actual sex, to further protect their identity. Additionally, the precise dates, times, quantities of narcotics, and dollar amounts of the sales are sometimes deliberately omitted to further obfuscate the CI's identity.

currency to make the arranged purchase.[3] At or near the same time, investigators established surveillance on Brewer Ave. Investigators then followed the CI to Brewer Avenue.[4]

12. Investigators conducting surveillance at Brewer Avenue saw a group of 4-5 individuals at the rear of the premises situated at 675/677 North Main Street. These individuals appeared to examine all vehicles entering Brewer Avenue, including the CI vehicle. Based on my training and experience, this behavior is consistent with individuals keeping a lookout to protect criminal activity from observation by law enforcement or threats by rival criminal organizations.

13. Investigators observed MILLER arrive at Brewer Avenue in the TARGET VEHICLE and approach the CI's vehicle. Soon thereafter, a Black male with a thin physical build, long dreadlocks styled hair, wearing a white T-shirt and khaki-colored shorts, later identified as Malcolm DESIR ("DESIR"),[5] approached. Investigators did not see where DESIR had come from. As he approached the CI and MILLER, who were now standing outside their respective vehicles, DESIR was observed carrying a black plastic bag that appeared to contain a rectangular object.

---

[3] The same pre and post controlled purchase procedure was employed with the CI for each of the controlled purchases.

[4] In each controlled purchase, the agents would meet with the CI beforehand, search the CI, and provide the CI with recording equipment and purchase money. The CI would then be followed to the meeting location. Investigators would also establish surveillance in the area that the purchase was to occur. During the purchase, agents would conduct surveillance and monitor the recording equipment. Following the sale, the investigators would follow the CI back to the meeting location where the CI would turn over the purchased items, would be debriefed about what occurred, and the recording equipment would be collected. These procedures were followed in each controlled purchase.

[5] Malcolm DESIR DOB XX/XX/1991 and SSN# XXX-XX-2512; goes by the street moniker "MALY" and is affiliated with the Flames Ville Legend Boys (FVLB) gang; who are known to hang out in the Ames Street areas, which includes Brewer Ave. DESIR is the subject of another Complaint and search warrant in connection with this same investigation.

14. Through both physical surveillance and the provided video equipment, investigators observed and monitored what followed. MILLER introduced DESIR to the CI and proceeded to explain to the CI that DESIR could supply the CI with narcotics, specifically cocaine. DESIR and MILLER both entered the CI's vehicle, DESIR in the front passenger seat and MILLER in the rear. DESIR was then observed reaching into the black plastic bag, retrieving, weighing, and packaging pressed[6] cocaine into another black plastic bag. DESIR then handed the CI the bag in exchange for a previously agreed-upon amount of money. DESIR also provided the CI with his phone number (XXX-XX2-0335) and informed the CI that DESIR could supply the CI with drugs when needed.

15. Investigators maintained surveillance on the CI while he returned to a prearranged location, recovered the electronic surveillance equipment, and removed from the CI's person a black plastic bag containing a hard white substance consistent in appearance with pressed cocaine. The substance was field tested and yielded a presumptive positive result for the presence of cocaine. The suspected cocaine weighed approximately 95 grams, including packaging. I reviewed the surveillance video of this transaction, and it appeared consistent with the CI's description of the controlled purchase.

[6] Cocaine is commonly trafficked in kilogram sized quantities in which the powder is compressed with considerable force into a solid brick-shaped object. Cocaine sold in smaller quantities that retains this pressed appearance can be indicative of a drug dealer in possession of a kilogram and 'chipping' the smaller quantities of cocaine off of the kilogram sized brick into the respective smaller quantities.

August 15, 2023 Firearm Purchase

16. On August 15, 2023, the CI contacted MILLER via cell phone number (XXX-XX5-0335)[7] and the social media platform Snapchat, under the username "GLOMANCJ[8]." These communications were recorded. The purpose of these communications was to negotiate the purchase of a firearm. MILLER agreed to sell a firearm to the CI and told the CI to meet him at 205 Plaistow Road Plaistow, NH 03865 (USA Storage).

17. Before conducting the controlled firearm purchase, investigators conducted surveillance at the TARGET RESIDENCE. The investigators witnessed MILLER departing from the TARGET RESIDENCE and thereafter entering the TARGET VEHICLE, which was observed to have no other occupants within. Approximately fifteen minutes later, MILLER initiated communication with the CI and indicated that he would arrive in thirty seconds. Investigators conducting surveillance at the purchase location witnessed the arrival of MILLER at USA Storage.

18. MILLER positioned the TARGET VEHICLE adjacent to the CI and directed him into a less populated section within the storage facility. MILLER instructed the CI to drive to the spaces between the storage units, obstructing visual observation from the road. Investigators observed the CI exit their vehicle and approach MILLER, who was positioned outside of the TARGET VEHICLE. The investigators witnessed MILLER approach the trunk of the TARGET VEHICLE and retrieve a firearm[9]. MILLER was observed showcasing the firearm to the CI,

---

[7] MILLER and DESIR own phone numbers with the same last four digits.

[8] MILLER furnished several different methods of communication to the CI, namely a cellular number (XXX-XX5-0335), the Snapchat account username "GLOMANCJ", and the Instagram account username “DEADGZ720.” Throughout the course of the investigation, the CI has employed all three methods of communication interchangeably in their interactions with MILLER.

[9] MILLER was not seen by investigators entering any storage locker at USA storage prior to the controlled purchase.

engaging in the action of removing and subsequently reinserting the magazine into the firearm. The magazine appeared to contain live ammunition based on investigators' observation of the video. MILLER provided the loaded firearm to the CI in exchange for the previously agreed price of $900.00 in U.S. currency.

19. Investigators subsequently recovered the firearm purchased from MILLER. The firearm has been positively identified as a semi-automatic Ruger handgun bearing the serial number 381-41552. The magazine was loaded with fourteen rounds of ammunition.

[redacted]

20. [redacted]

[redacted]

[redacted]

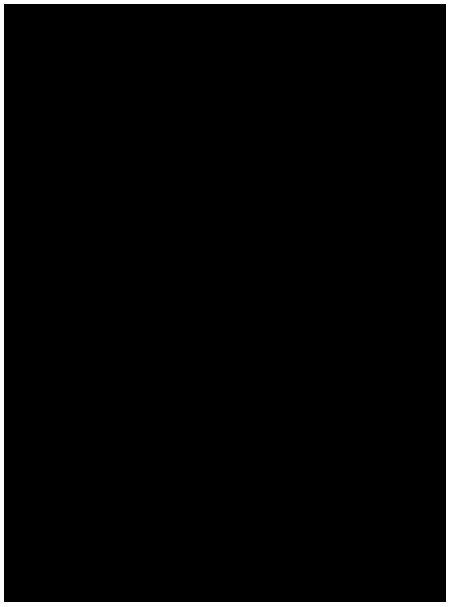
19. [redacted]

[redacted]

[redacted]

[redacted]

20. [redacted]



21. [redacted]

22. [redacted]

23. [redacted]

24. [redacted]

[redacted]

11 [redacted]

e) [redacted]

[redacted]

[redacted]

INSTALLED GPS ACTIVITIES/NOTATIONS

27. Over the course of a 45-day period beginning in September 2023 and going into October 2023, a Global Positioning System (GPS) tracking device has been affixed to a dark grey 2020 Honda Civic belonging to MILLER, bearing MA registration 9YE112 and Vehicle Identification Number (VIN) 2HGF22F69LH534981 (TARGET VEHICLE). The TARGET VEHICLE has consistently been parked in close proximity to 85 Evergreen Drive, Haverhill, during the majority of evenings, overnights, and mornings. This is the same vehicle that MILLER was observed driving from his place of residence to the first controlled purchase of a firearm at USA Storage (Plaistow, New Hampshire).

28. The investigators visited USA Storage and spoke with the management. They advised investigators that the only way to enter the facility is with an access card, which only those renting the units have. They then informed the Affiant that MILLER has been renting a storage unit at the property since June 12, 2023. The manager additionally furnished the investigator with a comprehensive record documenting each instance in which MILLER has accessed and departed from the USA Storage facility at 205 Plaistow Road, Plaistow, NH. On average, MILLER visits USA storage four times per week, occasionally making two visits in a single day. Information from

the GPS tracker installed in MILLER's vehicle aligns with the access information provided by USA Storage.

Use of Residences by Those Distributing Firearms and Narcotics

29. Through my training, experience, debriefings with firearm traffickers, and consultation with other special agents and law enforcement officers, I have learned that:

a. Individuals involved in firearm trafficking maintain documents and other records related to their illicit business at their residence and locations associated with them, including stash houses where they store their drugs. Specifically, individuals involved in drug trafficking often maintain ledgers in order to keep track of the purchasing, storage, distribution, and transportation of drugs and/or the laundering of the proceeds of their drug sales. Even after the drugs are sold and/or used, documentary records and ledgers are often maintained for long periods of time to memorialize past transactions and to maintain the names, telephone numbers, and contact information for suppliers, customers, and coconspirators.

b. Individuals involved in drug trafficking must often rely on others to obtain their drugs and/or the materials necessary to manufacture/distribute their drugs. In this case MILLER arranged for the CI to purchase cocaine from DESIR. Frequently, drug traffickers maintain evidence of the identities of these coconspirators at premises associated with them and will maintain these types of materials even after drugs are sold or used.

c. Individuals involved in firearm trafficking often take photographs of themselves, their associates, their property, and their firearms. Drug traffickers often take photographs of themselves, their associates, their property, and their controlled substances. Therefore, I am requesting permission to search for and seize photographs that law enforcement agents

determine to be of evidentiary value. In addition, in this case, screen captures were transmitted in furtherance of the sales.

d. Individuals involved in drug trafficking use various tools, instruments, materials, and other paraphernalia to facilitate their trafficking, including weighing the drugs, packaging the drugs, and cutting the drugs. These types of materials include but are not limited to, scales, cutting materials, and packaging materials. These types of materials are often maintained at locations associated with drug traffickers, even after drugs are sold or used.

e. I am also aware that it is generally a common practice for drug and firearm traffickers to conceal at their residences large sums of money, either the proceeds from drug/firearm sales or monies to be used to purchase firearms/controlled substances. Traffickers may use money transfer apps, wire transfers, cashier's checks, and money orders to pay for, and received payment for, firearms and controlled substances. Evidence of such financial transactions and records relating to income and expenditures of money and wealth in connection with drug and firearm trafficking would also typically be maintained in residences.

f. Individuals involved in firearm trafficking often keep weapons, including firearms, at the locations where they store their drug supplies in order to protect both themselves and their drugs from thefts and/or robberies.

g. Based upon my training and experience as a law enforcement officer, I know that individuals typically possess in their residences documents and other items that reflect their occupancy and control of the premises, such as but not limited to personal mail, checkbooks, identification, notes, correspondence, leases, utility bills, rent receipts, financial documents, keys, and photographs.

30. On August 15, 2023, investigators saw MILLER leave the TARGET RESIDENCE at 85 Evergreen Drive, Haverhill. Investigators observed MILLER, maintaining visual contact with him throughout his traveled route until he arrived at USA Storage. MILLER then engaged in a firearm transaction with the CI without being seen to access any storage containers. Based on the foregoing, there is probable cause to believe that the firearm had been kept at the TARGET RESIDENCE prior to the sale. Similarly, following the second controlled firearm purchase, MILLER was followed from the location of the sale back to the TARGET RESIDENCE.

SEIZURE OF COMPUTER EQUIPMENT

Use of Cell Phones by Those Distributing Narcotics and Firearms; Probable Cause to Believe MILLER's Cell Phone(s) Will Contain Evidence of the Target Offense

31. Based upon the foregoing, there is probable cause to believe that MILLER and co-conspirators used cellphones and social media applications to communicate in furtherance of cocaine and firearms sales. Based on my training and experience, I know that records relating to these communications are likely stored on MILLER's phone.

32. I am aware that, according to the Pew Research Center, as of 2021, 97 percent of adult Americans own a cellphone, and 85 percent own a smartphone. The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29-year-olds and 95 percent of 30-49-year-olds owned smartphones in 2021. MILLER is currently 27 years old.

33. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computer equipment, including smartphones, to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; arranging for travel; taking and storing pictures;

researching topics of interest; buying and selling items; and accessing their bank, financial, investment, utility, and other accounts online. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer equipment, including smartphones.

34. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

35. Based on my experience and training, I know that individuals who own and possess cell phones normally possess and maintain them for reasonably long periods of time because they are expensive, can often be subject to long-term contracts that contain substantial penalties for early termination, can store large amounts of information, and do not easily wear out.

36. In my experience, cell phones are most often maintained by the user on his person or in his residence when not outside.

37. Based on my knowledge, training, experience, and information provided to me by other agents, I know that data can often be recovered months or even years after it has been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their electronic equipment, they can easily transfer the data from their old device to a new one.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, the device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media often contains electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store

configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify the records to be sought in advance,

computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

38. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence - storage media such as hard disks, flash drives,

CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities

of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements - analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap." Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

39. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B, are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents,

regardless of how the contents or ownership appear or are described by people at the scene of the search.

40. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) MILLER. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

41. I know from my training and experience, as well as from information found in publicly available materials, that some models of cell phones made by Apple and other manufacturers offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

42. On Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) on the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as (1) when more than 48 hours have passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours, and the passcode or password has not been entered in the last six days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch

ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted, (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

43. The passcode that would unlock the devices found during the search of the TARGET RESIDENCE is not currently known to law enforcement. Thus, it may be useful to press finger(s) of MILLER to the fingerprint sensor of the devices found during the search of the TARGET RESIDENCE or to hold the devices up to MILLER's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

44. For these reasons, I request that the Court authorize law enforcement to press fingers (including thumbs) of MILLER to the sensor of the devices found at the TARGET RESIDENCE, TARGET VEHICLE and/or MILLER's person or place the devices in front of his face for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

CONCLUSION

45. Based on the foregoing, there is probable cause to believe that MILLER participated in the sales of cocaine and multiple firearms. MILLER is not licensed to sell or possess firearms, and he facilitated the sale of firearms to an individual he knew to be prohibited from possession of firearms as a convicted felon. Furthermore, MILLER has personally engaged in the unlawful possession and sale of a firearm to a confidential informant (CI). Accordingly, there is probable cause that MILLER violated Title 21, United States Code, Sections 841(a)(1) and 846 - distribution of and possession with intent to distribute controlled substances, and conspiracy to do

the same; Title 18, United States Code, Section 933 – trafficking in firearms, and Title 18, United States Code, Section 922(g)(1) – possession of a firearm by a felon, and Title 18, United States Code, Section 2 – aiding and abetting (TARGET OFFENSES).

46. I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the person of MILLER, the TARGET RESIDENCE, and the TARGET VEHICLE described in Attachments A-1, A-2, and A-3.

Sworn to under the pains and penalties of perjury,

John Moynihan

Det. John T. Moynihan
Task Force Officer, ATF

Sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 on this Nov 1, 2023 the Day of November 2023.

Judith Gail Dein

HON. JUDITH G. DEIN
UNITED STATES MAGISTRATE JUDGE